COVID-19
and Data Rights in Uganda

April **2022**

CIPESA

Table of Contents

CIPESA acknowledges the contribution of Paul Kimumwe, Edrine Wanyama, Victor Kapiyo, and Wakabi Wairagala in the writing of this report.

The report was produced with support from the Hewlett Foundation in the context of promoting data openness among public and private actors, and advancing respect for data rights towards citizens' participation and informed policy decisions in rights-respecting data-for-development initiatives.

Introduction

The fight against the coronavirus (COVID-19) pandemic in Uganda dealt a blow to the enjoyment of digital rights. From the on-set of COVID-19 responses, there was a significant increase in the collection and processing of personal data as the government traced persons suspected to have contracted or been exposed to the virus. As part of efforts to combat COVID-19, the government passed various regulations that provided the legal basis for contact tracing. These included the Public Health (Control of COVID-19) Rules, 2020 under the Public Health Act,[1] which gave medical officers and health inspectors powers to enter any premises to search for cases of COVID-19, and to order the quarantine or isolation of all contacts of the suspected COVID-19 patients. Another was the Public Health (Prevention of COVID-19) (Requirements and Conditions of Entry into Uganda) Order,[2] 2020 which allows a medical officer to examine for COVID–19, any person arriving in Uganda. There are additional Guidelines[3] on Quarantine of Individuals which required all quarantined persons to provide their name, physical address, and telephone contact to the health ministry monitoring team.

In March 2020, the government embarked on a contact tracing[4] exercise of persons entering the country for testing and possible quarantine. The health ministry stated that it was in possession of contact details[5] of all returnees, which it was using to trace them. The private data collection and conduct of surveillance appear to have lacked sufficient oversight, safeguards, or transparency. And in what appears to be a breach of individual privacy, there were reports of some Ugandans using online platforms, mainly Facebook and WhatsApp, to share personal contact details of the suspected returnees, with threats of further exposure should they fail to report for testing. This led to some returnees being targeted with physical attacks,[6] being threatened with eviction[7] and online exposure that breached their rights to privacy as provided for in the Data Protection and Privacy Act, 2019.[8]

The Data Protection and Privacy Act 2019 seeks to protect the privacy of individuals by regulating the collection and processing of personal information. It also provides for the rights of the persons whose data is collected and the obligations of data collectors, data processors, and data controllers; and regulates the use or disclosure of personal information. Following the outbreak of the COVID-19 pandemic, poor data governance practices right from when the government was tracing the COVID-19 contact persons were witnessed, with peoples' data being collected and processed without following the law.

1 *https://covidlawlab.org/wp-content/uploads/2021/02/Public-Health-Control-of-COVID-19-No2-Rules-2020.pdf*

2 *https://covidlawlab.org/wp-content/uploads/2021/02/Public-Health-Prevention-of-COVID-19-Requirements-and-Conditions-of-entry-into-Uganda-Order-2020.pdf*

3 *https://www.health.go.ug/covid/wp-content/uploads/2020/04/Updated-Guide-Draft_24April20_CLEAN.pdf*

4 *https://www.monitor.co.ug/News/National/Coronavirus--Uganda-hunts-500-Dubai-returnees/688334-5505194-6ysp01z/index.html*

5 *https://www.monitor.co.ug/News/National/Coronavirus--Uganda-hunts-500-Dubai-returnees/688334-5505194-6ysp01z/index.html*

6 *https://ekyooto.co.uk/2020/04/02/covid-19-kyengera-mob-lynches-dubai-returnee/*

7 *https://www.monitor.co.ug/News/National/Dubai-returnee-wife-quarantined-Jinja-Hospital-threaten-eviction/688334-5502558-r8ynhpz/index.html*

8 *https://ulii.org/system/files/legislation/act/2019/1/THE%20DATA%20PROTECTION%20AND%20PRIVACY%20BILL%20-%20ASSENTED.pdf*

This research seeks to discuss the key digital rights issues, policies and programs around Uganda's fight against COVID-19 and how these may have affected citizens' trust in government, and in protecting their personal data. The study also explores the challenges that data intermediaries and public institutions face in engendering responsible data governance practices during crises like the COVID-19 pandemic.

Research Methodology

The study employed a combination of qualitative data collection tools, including a review of relevant literature such as reports, media reports, laws, and policies like guidelines on privacy and personal data as well as the COVID-19 response measures by the government.

In addition, the research conducted key informant interviews with purposively selected respondents. Purposively selected respondents had knowledge and expertise in data governance issues and COVID-19 response data management. The literature review and key informant interviews were guided by the following questions.

1. How effective was the existing legislation in guiding government actions on collection and use of COVID-19 data?
2. Did government agencies adhere to the data protection principles in the collection and use of COVID-19 data?
3. What were the common personal data privacy concerns in the handling of COVID-19 in Uganda?
4. How did the handling of COVID-19 data influence perceptions on data risks and safety?
5. How can data governance be improved during crises such as COVID-19?
6. How can governments harness data to inform policy and decision making while protecting digital rights?

Data Protection **and Privacy in Uganda**

The right to privacy is provided for under article 27 of the Constitution. Article 27 states that:

1) No person shall be subjected to—
- *a)* unlawful search of the person, home, or other property of that person; or
- *b)* unlawful entry by others [into] the premises of that person.

2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication, or other property.

The right was further buttressed in 2019, with the enactment of the Data Protection and Privacy Act, 2019. The Act provides for the protection of privacy of the individual and of personal data by regulating the collection and processing of personal information. It also provides for the legal rights of persons whose data is collected and the obligations of data collectors, data processors and data controllers, as well as regulating the use or disclosure of personal information.[9] In May 2021, the government adopted the Data Protection and Privacy Regulations to operationalise the Act.[10]

Surveillance and Personal Data Collection in Uganda

For decades, personal data was collected for security reasons on the basis of section 3 of the Security Organisations Act of 1987 and section 19(6)(a) of the Anti-Terrorism Act. The Citizenship and Immigration Control Act[11] also formed a basis to gather information and data on individuals applying and acquiring passports and those entering and leaving the country.

In 2015, government passed the Registration of Persons Act, 2015[12] to harmonise and consolidate the law on registration of persons and provide for establishment of a national identification register, and establish the National Registration and Identification Authority. It also provides for the issuance of national identification cards and aliens identification cards.

9 *Uganda Data Protection and Privacy Act, 2019 https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf*

10 *The Data Protection and Privacy Regulations, 2021, https://www.dataguidance.com/sites/default/files/uganda_data_protection_regulations_small.pdf*

11 *Citizenship and Immigration Control Act, https://www.mia.go.ug/sites/default/files/download/The%20Uganda%20Citizenship_Immigration_Control%20Act.pdf*

12 *Registration of Persons Act, 2015 https://www.ict.go.ug/wp-content/uploads/2018/06/Registration-of-Person-Act-2015.pdf*

The National Identification and Registration Authority (NIRA) is established under section 4 of the Act and its functions under section 5 of the Act include to create, manage, maintain, and operate the National Identification Register and to register citizens and non-citizens who are lawfully resident in Uganda. According to Schedule 3 of the Act, those registering are required to provide the following information: name and date of birth, citizenship and details of the citizenship, place of birth, details of parents, clan, descendants, tribe, ethnicity, sex, marital status, details of spouse where applicable, education and profession, occupation, address, and tax identification numbers.

Section 9(2) of the Regulation of Interception of Communications Act, 2010 required telecommunication service providers to ensure that existing subscribers register their SIM cards within six months from the date of commencement of the Act. The registration of SIM cards was made mandatory in Uganda in 2012.[13]

Uganda has developed a Biometric Voter Verification System (BVVS) through which fingerprints and images of all registered voters are collected. In the 2016 elections, voters' records relating to more than 15.27 million individuals were sourced from the National Security Information System, which is managed by the National Identification and Registration Authority (NIRA) and is the basis for issuing national IDs.[14] The BVVS uses fingerprints to match voter details to confirm that the person is on the voters' roll for a given polling station. The data in the BVVs includes the name, place and date of birth, location of the polling station and fingerprints of the voter. The BVVS was also used in the 2021 elections, effectively disenfranchising citizens who did not possess national IDs.[15]

In addition, the government has boosted its surveillance capacity through enactment of several enabling laws and the acquisition and deployment of relevant software. For example, in 2012, it enhanced its mass surveillance capacity using spyware, intrusion malware, and intelligent network monitoring systems.[16] In July 2018, the Uganda communications regulator, Uganda Communications Commission (UCC), was reported to have installed an Intelligent Network Monitoring System (INMS) with the capacity to track all calls made on all networks, mobile money transactions, fraud detection and billing verification.[17]

The Anti-Terrorism Act in Part VII (sections 18 to 22) provides for the interception of communications and surveillance on grounds such as the public interest, national economy and security, prevention of crime and protection of human rights and freedoms. Part VII of this law has been reinforced by section 2 of the Regulation of Interception of Communications Act which provides for control of interception. Section 11 of the Act requires intermediaries such as telecom companies and Internet Service Providers (ISPs) to facilitate surveillance including by installing equipment and software that enable the government to lawfully intercept communications on their networks, including in real-time for such periods as may be required. The failure to comply with the requirement to support interception attracts a fine of UGX 2 million (USD 563), imprisonment for a period not exceeding five years, or both. In addition, section 28 of the Computer Misuse Act provides for searches and seizures by state security agencies, which potentially facilitates surveillance on the activities of individuals.

.

13 *New Vision (2012) SIM Card registration kicks off in March, https://www.newvision.co.ug/news/1298713/sim-card-registration-kicks-march*

14 *The Electoral Commission, 2015/2016 General Elections Report, https://www.ec.or.ug/docs/Report%20on%20the%202015-2016%20General%20Elections.pdf*

15 *Millions May Miss Voting Over National IDS - EC, https://www.monitor.co.ug/SpecialReports/Elections/Millions-may-miss-voting-over-national-IDs---EC/-/859108/2983320/-/13im600/-/index.htm*

16 *State of Privacy Uganda, https://privacyinternational.org/state-privacy/1013/state-privacy-uganda#commssurveillance*

17 *ITWeb Africa, Uganda's UCC, telcos clash over network monitoring technology, https://bt.ly/2NEMVON*

COVID-19 Fallout and Data Rights in Uganda

In an effort to contain the spread and mitigate the effects of COVID-19, the government undertook several measures including the adoption and implementation of several statutory instruments which provided the legal basis for contact tracing.[18] These included the Public Health (Control of COVID-19) Rules, 2020 under the Public Health Act Cap.281, which gave powers to a medical officer or a health inspector to enter any premises in order to search for any cases of COVID-19 or inquire whether there is or has been on the premises, any cases of COVID-19.[19] Additionally, rule 5 empowers a medical officer of health to order the quarantine or isolation of all contacts of the suspected COVID-19 patients.

The Public Health (Prevention of COVID-19) (Requirements and Conditions of Entry into Uganda) Order, 2020 allows a medical officer of health to examine for COVID–19, any person arriving in Uganda and may, for this purpose, enter upon or board any vehicle, aircraft or vessel arriving in Uganda and examine any person on board the vehicle, aircraft, or vessel.[20]

The extent of data collection and the methods used to collect data for COVID-19 contact tracing and surveillance is not fully known. Besides government's secrecy on this, it is apparent that several government entities were involved in data collection, or deployed tools for this purpose. Even though the health ministry was the national coordinator of efforts to combat COVID-19, it is not clear that all data collection efforts were under its wing or whether other entities collaborated with the health ministry.

The implementation of the public health regulations raised several issues regarding privacy and data rights. First, there is no evidence to indicate that there were diverse consultations before their adoption. In addition, sections of the public questioned the legal basis of the presidential directives which informed the wording of the regulations.[21]

There were also concerns that the regulations were in breach of the data protection principles[22] provided for in the Data Protection and Privacy Act as well as other international human rights instruments. Principles such as accountability and transparency, fairness and lawfulness, quality control and storage limitation on data retention and observing security safeguards such as data integrity and confidentiality appear to not have been adequately addressed. In addition, data subjects' rights, including preventing the processing of personal information, rectification and erasure, restriction on processing and automated decision making were not well observed.[23] These rights should be protected and respected by all data processors and controllers to ensure the relevant privacy guarantees.

Evidentially, the collection, processing, use and sharing of COVID-19 information especially through contact tracing can help in limiting the spread of the virus since it enables monitoring to track the spread and potential spread of the virus.[24] The processes must, however, be exercised with caution to ensure that human rights, specifically data protection and privacy, are complied with through adherence to data rights and principles. However, in many countries across the world there was no clear mechanism from developers and the government that the COVID19 tracking applications' side effects on personal data protection would be avoided or minimised.[25] In Uganda, as is explained below, key data rights concerns emerged.

18 *State of Internet Freedom in Africa 2020: Resetting Digital Rights Amidst The COVID-19 Fallout https://cipesa.org/wp-content/uploads/2021/04/The-State-of-Internet-Freedom-in-Africa-2020-Report.pdf*

19 *Section 6(1) of the Public Health (Control of COVID-19) Rules of 2020 https://ulii.org/ug/legislation/statutory-instrument/2020/52*

20 *Section 2 of The Public Health (Prevention of COVID - 19) (Requirements and Conditions of Entry into Uganda) Order, 2020 https://ulii.org/ug/legislation/statutory-instrument/2020/46*

21 *Parliament demands statutory instruments on COVID-19 directives https://www.independent.co.ug/parliament-demands-statutory-iistruments-on-covid-19-directives/*

22 *Section 3 of the Data Protection Act, 2019.*

23 *Sections 24-28 of the Data Protection Act, 2019 explains the range of such rights; see also Chapter 3 (articles 12-23) of the General Data Protection Regulation, https://gdpr-info.eu/*

24 *WHO, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing," May 28, 2020, https://apps.who.int/iris/rest/bitstreams/1278803/retrieve*

25 *OECD, "OECD Policy Responses to Coronavirus (COVID-19): Ensuring data privacy as we battle COVID-19," April 14, 2020, https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/*

Unenforced COVID-19 Data Collection Regulations

By the time the government intensified its COVID-19 contact tracing, Uganda had a data protection law enacted in 2019 whose implementing regulations would only come into force in mid-2021. Nonetheless, the National Information Technology Authority (NITA-U) developed a privacy policy for the COVID-19 tracing app developed by the Ministry of Health and NITA-U[26] [27] but accessing the policy on NITA-U's website requires prior authorisation.[28] The requirement for "prior authorisation" to access a document held by a public body, which has not been classified as an "exempt record", runs counter to the proactive disclosure of information practices under international law and Uganda's Access to Information Act, 2005. Additionally, "this authorisation requirement suggests that NITA-U failed to fully respect the public's right to know.

Besides concerns about the public availability of the policy and the need for prior authorisation, a separate issue is whether these guidelines were implemented. To-date, the Ministry of Health, NITA-U and other entities that run contact tracing applications have not provided any public information on what and how much was collected, where it is stored, how it was utilised, and if the apps have since been discontinued. Since NITA-U is the statutory authority which, according to section 3(2) of the Data Protection and Privacy Act, is responsible for collection, control and processing of personal data and the custodian of the national data protection register, it was imperative that it issued guidelines to govern all COVID-19 related data collection and use, and not just for the app it helped to found. Moreover, NITA-U should have monitored how the various apps and government departments and private companies such as telecom service providers were collecting, storing and using data, and whether their practices were in conformity with the country's laws and international best practice.

26 Trace Uganda Privacy Policy, https://www.nita.go.ug/media/trace-uganda-privacy-policy

27 One Trust Data Guidance, Uganda: NITA-U publishes tracing app privacy policy, 21 May 2020.

28 NITA-U, Privacy Policy.

Disregard for Data Protection Principles

Section 3 of Uganda's Data Protection and Privacy Act provides for several principles of data protection under subsection 1. It states that a data collector, processor or controller or any person who collects, processes, holds, or uses personal data shall:

a) Be accountable to the data subject for data collected, processed, held, or used;
b) Collect and processes data fairly and lawfully;
c) Collect, process, use, or hold adequate, relevant, and not excessive or unnecessary personal data;
d) Retain personal data for the period authorised by law or for which the data is required;
e) Ensure quality of information collected, processed, used, or held;
f) Ensure transparency and participation of the data subject in the collecting, processing, use and holding of the personal data; and
g) Observe security safeguards in respect of the data.

Under section 3(2), NITA-U is required to ensure that every data collector, data controller, data processor or any other person collecting, or processing data complies with the principles of data protection and this Act.

Unfortunately, several measures adopted by the state did not meet the minimum threshold of principles of data protection principles. For example, one of the requirements for the resumption of work by motorcycle transporters (commonly known as boda bodas), was for them to collect data and keep a register of all their customers, including names, phone numbers, temperature, and destination.[29] In Uganda boda bodas are notorious for various unsavoury behaviours including cooperating with robbers and disregard for the law. Handing them power to collect data and be responsible for its safe storage, without any guidance on how to do so, how long to keep the data, where to take the data they collected, were critical breaches to best practice. According to several respondents, various data subjects' rights were breached in the process.

> *"There were no clear guidelines on how the data would be collected, stored, and kept safely. In addition, there were gaps on how the data that was to be collected by entities such as boda boda riders of their clients would be processed, and shared and kept safe,"* according to Moses Owinyi.

On his part, Bernard Sabiti noted that there were no guarantees to protect patients' data as there was no clear data protection plan in place. According to him, in future this will make people sceptical when asked to provide personal data, even in the event of an emergency. "People's COVID-19 status were open for reveal and shaming; Telephone numbers, NINs [National Identification Numbers] given for COVID relief; boda bodas [collecting data], etc. So, a person was vulnerable to identity theft, and cyber financial crimes," he added.

According to a traveller who returned to the country just before the international space was closed, all passengers were required to fill a physical form with details of where they would stay, their telephone contact and that of next of kin.[30] Travellers were also required to fill a form indicating where they were coming from, if at all they had come into contact with a person who had COVID-19. They had to indicate if they had symptoms of COVID-19 like flu, cough, and fever. They were also asked to provide their phone numbers and emails.[31]

---

29 *Ugandan Boda Bodas Return to Road – With Requirements https://www.voanews.com/a/africa_ugandan-boda-bodas-return-road-requirements/6193508.html*

30 *Dr. Emily Maractho, Daily Monitor (2020) Ministry of Health should check its current confidence on COVID-19; https://www.monitor.co.ug/OpEd/Commentary/Ministry-of-Health-current-confidence-on-COVID19/689364-5522462-hws4rs/index.html*

31 *Interview with Dr. Jimmy Spire Sentongo*

Breach of Privacy and Confidentiality

While early in the pandemic the health ministry used to trace and isolate whoever came into contact with a confirmed positive or suspected case, a model borrowed from Ebola surveillance, Dr. Charles Olaro, the Director Clinical Services, says their contact tracing system got skewed when community infections became rampant.[32] In addition, as the number of cases rose and the government doubled its efforts to reach out to the increasing number of returnees for further testing, especially those who had been allowed to go home,[33] there were reports of Ugandans using online platforms, mainly Facebook and Whatsapp, to share personal contact details of the suspected returnees, with threats of further exposure should they fail to report for testing.

Messages such as those below were circulated on social media, accompanied by threats of exposure of the affected individuals.

> ***"MK. You were working as a cleaning supervisor in (name of shopping mall withheld). You are now in (name of area withheld) chilling."***

> ***"……. B.H, a decorator at (name of build withheld) in Kisekka. You went to Dubai to buy (type of goods withheld) for your company (company name withheld) and came back on 13th March. You are now hiding at your father's home in (name of the area withheld)"***

> ***"…… N. You were in Dubai this month. Your phone number ends with 492. You know yourself "***

There were also reported cases of threats of and actions of violence against individuals suspected to be returnees by the community.[34] The Ministry of Health was reported to be in possession of the details of all passengers who had entered the country in the second and third weeks of March 2020, which details the ministry was using to trace them.[35] However, it was not clear what measures the ministry and other authorised data collectors and processors had undertaken to ensure the safety and confidentiality of contacts' personal data.

32 *https://www.independent.co.ug/health-ministry-stops-tracing-covid-19-patient-contacts/*

32 *Coronavirus: Uganda hunts 500 Dubai returnees https://www.monitor.co.ug/News/National/Coronavirus--Uganda-hunts-500-Dubai-returnees/688334-5505194-6ysp01z/index.html*

34 *COVID-19: Kyengera mob lynches Dubai returnee https://ekyooto.co.uk/2020/04/02/covid-19-kyengera-mob-lynches-dubai-returnee/; see also; COVID-19: Dubai returnee, wife quarantined at Jinja Hospital after residents threaten with eviction https://www.monitor.co.ug/News/National/Dubai-returnee-wife-quarantined-Jinja-Hospital-threaten-eviction/688334-5502558-r8ynhpz/index.html*

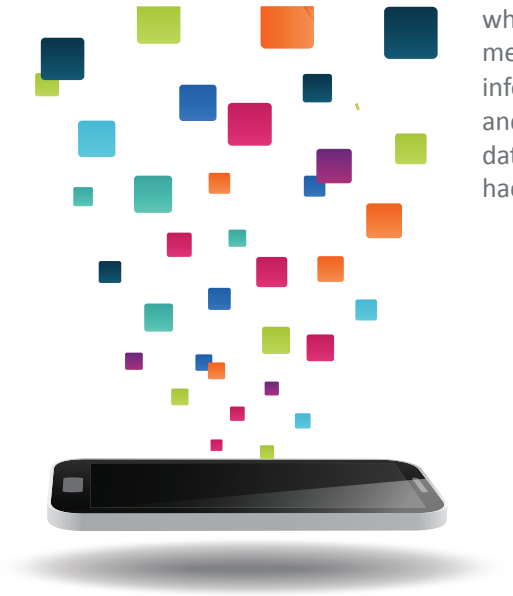
35 *Ibid*

Unmitigated Multiplicity of Apps and lack of Transparency

The development and application of various unproven technologies and mobile applications to support contact tracing raised several data privacy rights issues as they increased the potential for abuse and presented risks for repurposing the technologies for mass surveillance after the pandemic.

Motivated by the need to trace those suspected to be infected with the virus and those who had come into contact with infected persons, the government and private entities initiated various technology applications. Applications such as the MTN-NITA Geolocation Tracing App, E-pass (Electronic Pass), was developed to aid tracking of those infected and suspected carriers.[36] Similarly, Makerere University developed the C-19 Mobile Contact Tracing App for similar purposes.[37] Among others, it would entail digitising investigating and contact tracing for COVID-19s. Furthermore, the ICT Ministry, MICT, CTI Africa app in May 2020 unveiled a "world class mobile app aimed at containing COVID-19"[38] that would facilitate remote patient diagnosis and instant notifications to the health ministry.

Further, in 2020 through the National ICT Initiatives Support Programme (NIISP) funding, Uganda developed the Cogniware Insights Epidemiology App to manage and apply protective measures such as "smart quarantine", isolation, and contact tracing. Meanwhile Defining Technology, a private entity, developed a contact tracing app to perform similar roles.[39]



Common to the developed applications is that personal data would be collected whether voluntarily or without consent. There was no clear data management mechanism. The development of the applications was a race against rising infections[40] and paid little attention to privacy guarantees, creating room for data and privacy breaches. Even then, accountability and transparency for collected data became difficult due to the multiplicity of contact tracing applications that had been deployed.

36 *Daily Monitor, "The new app named E-pass (Electronic Pass) is intended to help the Ministry of Health track and geo-fence the movement of COVID-19 patients," https://www.monitor.co.ug/uganda/brand-book/mtn-uganda-and-nita-uganda-launch-new-app-for-tracking-covid-19-patients-under-home-based-care-3331474*

37 *Mark Wamai, "Mak Unveils C-19: COVID-19 Mobile Contact Tracing App," April 1, 2021, https://news.mak.ac.ug/2021/04/mak-unveils-c-19-covid-19-mobile-contact-tracing-app/*

38 *Ministry of Health, "Government of Uganda Launches Mobile COVID-19 Application," https://www.health.go.ug/2020/05/28/government-of-uganda-launches-mobile-covid-19-application/*

39 *Harnessing digital innovations under the COVID-19 pandemic: A case of Uganda's ICT sector, https://www.finance.go.ug/sites/default/files/Publications/BMAU%20Briefing%20Paper%207-20-Harnessing%20Digital%20Innovations%20under%20COVID-19%20pandemic.%20A%20case%20of%20Uganda%25u2019s%20ICT%20sector.pdf*

40 *COVID-19 Interventions Report, 2019/20, https://covid19.gou.go.ug/uploads/document_repository/authors/minstry_of_finance,planning_and_economic_development/document/COVID-19_Interventions_Report.pdf*

The MTN-NITA Geolocation Tracing App: The telecom company MTN Uganda and NITA-U developed an app called E-pass (Electronic Pass)[41] which they said would be used "to help the Ministry of Health track and geo-fence the movement of COVID-19 patients" that were under home-based care, "thus reducing the number of non-critical patients that get admitted in hospitals." According to MTN, development of the app lasted four months and cost UGX 460 million (USD 130,000). It was handed to the health ministry along with 400 smartphone handsets installed with the app that would be used for monitoring. This app utilised monitoring geo-location of individuals and their movements. The General Manager for MTN Business, Ibrahim Ssenyonga, said the app would help the government to better manage resources as non-critical patients could now be monitored remotely from their locations of isolation. The MTN official said: "This new app will alert the ministry of health designated officials in case a patient under surveillance goes outside of the planned location boundaries. That way, the ministry can minimise further spread, but also be able to locate some of the contacts in the areas where the patient might have veered off to." The NITA-U Executive Director said the solution would be a "game-changer in managing the COVID-19 pandemic", while the health ministry Permanent Secretary said it would solve the problem of people who did not need to be in health centres going to the facilities and taking up space for those that needed to be there the most. Atwine said the solution was "a win for us as a country in the management of this pandemic."

The ICT Ministry, MICT, CTI Africa App: In May 2020, the health ministry announced that the ICT ministry with support from Ugandan developers CTI-Africa had developed and launched a "world class mobile app that shall be used to help in curbing the spread of COVID-19."[42] The "Call the Clinic" (MOH - CTC) app would "facilitate remote patient diagnosis and instant MOH notifications." The app would help the government's objective for symptomatic patients to have immediate access to health agents via voice and video call. A patient using android could download the app from Google Play or access the link on the Ministry of Health website, register their credentials, then access a welcome screen to call the clinic (CTC). With the information provided, doctors could remotely diagnose patients. The ministry said individuals would also access informative and educative information from the health ministry on the latest updates and statistics. Moreover, through the application, "the local community is able to send anonymous notifications of local symptomatic patients."

The Makerere University C-19 Mobile Contact Tracing App: Makerere University researchers announced they had developed a mobile application that digitises the investigation, case, and contact tracing for COVID-19 in communities.[43] With funding from Makerere University Research and Innovations Fund (MakRIF) and in partnership with the Child and Family Foundation Uganda and Ministry of Health, the application was designed "to investigate case and contact tracing for COVID-19, timely reporting and decision making to improve the efficiency of COVID-19 response and capture community feedback." As part of the features, the application has various COVID-19 self-assessment components on its Epi-COVID Tracer Dashboard. This enables the app user to undergo self-screening or screen others using different prompts. The application, according to March 30, 2021 information, "also boasts of support services that include COVID-19 Laboratories and hospitals all authorised by the Ministry of Health. One can consult Private Doctors and Counsellors on the App through WhatsApp or other call options."

The developers were inspired by the need to address the existing challenges of trekking long distances for hours to ascertain information regarding suspected or confirmed cases of COVID-19, delayed communication and responses, loss of contact lists and transcription errors. They explained: "Currently, community surveillance teams have to trek distances for hours to go and find information from suspected or even confirmed cases. Therefore, challenges such as incomplete identification of contacts, delays in communication, and response, loss of contact lists, inadequate data collection, and transcription errors exist, making the system slow, and inefficient. Thus, information exchange between involved parties is too slow and expensive because, by the time a response is generated, the disease is spreading."

---

41 https://www.monitor.co.ug/uganda/brand-book/mtn-uganda-and-nita-uganda-launch-new-app-for-tracking-covid-19-patients-under-home-based-care-3331474

42 https://www.health.go.ug/2020/05/28/government-of-uganda-launches-mobile-covid-19-application/

43 https://news.mak.ac.ug/2021/04/mak-unveils-c-19-covid-19-mobile-contact-tracing-app/

The ICT Ministry Funded COVID Apps: Among the innovations Uganda announced that had won funding under the 2020 National ICT Initiatives Support Programme (https://niisp.ict.go.ug/2020-award) is Cogniware Insights Epidemiology App, an open platform to manage and apply protective measures such as "smart quarantine", isolation and contact tracing; COVID19 Data Engine, a system to collect and analyse COVID-related data; COVidTrace App, which records and analyses user movement data; Surveillance tracing and follow up system for COVID, which digitises the identification and tracing of COVID-19 suspects and cases as well as their contacts; and Uganda Health Survey Geographical Information Systems, a digital system for surveillance of COVID-19 pandemic cases and other diseases of public health concern.

Defining Technologies' COVID Tracer: Defining Technology, a Ugandan firm, developed a contact tracing app which it said alerted users and the Ministry of Health "in case someone has been in contact with a COVID-19 positive person using Geographic Positioning System (GPS) and Bluetooth capabilities in a smartphone." By May 2020, promoters of the app said more than 5,000 users had signed up on the app, and that the app had been donated to the Ministry of Health National Taskforce to help in fast tracking of contacts.[44] According to an official description, the digital contact tracing app uses overlapped GPS and Bluetooth trails that allow an individual to check if they have crossed paths with someone who was later diagnosed with the virus. Meanwhile, through COVID Tracer, public health officials "are equipped to redact location trails of diagnosed carriers and thus broadcast location information with privacy protection for both diagnosed patients and local businesses." Using the Bluetooth capabilities in smartphones, the COVID-19 Tracing app kept records of who a person met and if a user or contact was confirmed to be positive, it would send notifications to everybody on that list, advising them to self-isolate.

"The public users can see if they have been exposed, privately log your location and completely control your data whereas the champions of this fight (public health officials) are offered with reliable contact tracing, map infections with accuracy and anonymously verify cases," said Toskin Gregory, a staff at Define Technologies. He said the app used smartphone technologies such as GPS and Bluetooth to collect and share the data, which are agile and easy to use.[45]

However, despite reports of close collaboration between state agencies and private actors to deploy digital technologies as part of pandemic measures, there is no transparency about these partnerships. While there have been press reports detailing collaboration on digital contact tracing initiatives, there is no publicly accessible information about public–private contracts, data sharing agreements, architecture of the technologies, budgetary allocations, or procurement processes of these pandemic surveillance technologies.[46] Moreover, it is not clear the amount of information that each of these apps collected including the number of data subjects involved. It is also not known if such information was inter-linked or has been centrally stored by the health ministry or other government department, or, indeed, whether some of the data has since been disposed of.

44 Harnessing digital innovations under the COVID-19 pandemic: A case of Uganda's ICT sector, https://www.finance.go.ug/sites/default/files/Publications/BMAU%20Briefing%20Paper%207-20-Harnessing%20Digital%20Innovations%20under%20COVID-19%20pandemic.%20A%20case%20of%20Uganda%25u2019s%20ICT%20sector.pdf

45 https://allafrica.com/stories/202005250236.html

46 https://www.article19.org/wp-content/uploads/2021/04/ADRF-Surveillance-Report-1.pdf

Conclusion

The fight against COVID-19 has been characterised by an assortment of measures that have resulted in the violation of privacy rights in Uganda. The International Covenant on Civil and Political Rights, which has been ratified by Uganda, provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence. However, in practice, the new COVID-19 legislation as well as pre-existing laws that were cited in implementing pandemic-related emergency measures, such as the searching of homes, collection of personal information of individuals, contact tracing and surveillance activity, went against this provision.

These measures mostly had the effect of undermining individuals' data rights, with some amounting to involuntary surrender of personal data yet measures to ensure the security of data collection, storage and processing were not clear or guaranteed.

Prior to COVID-19, the government had already enhanced its surveillance capacity through enacting the enabling legal framework, as well as engaging in massive collection of personal data, aided by imports of technology and expertise from more technologically developed countries including China. While surveillance is permitted in Uganda's laws and policies, the risk expressed before COVID-19 was that the practice could increasingly go unchecked as the technologies become more sophisticated, harder to detect and widespread.[47] This surveillance activity has often been undertaken with limited oversight and often to target those legitimately expressing opinions critical of their leaders.

For citizens to have the confidence to participate in government digitalisation programmes, particularly those that involve collecting their data, they should have trust that the privacy of their data will be upheld. Further, they need to have confidence that data collectors and processors will not use that data to abuse their digital rights, such as by conducting surveillance against them or exposing them to scams and cyber criminals. Notably, individuals' identification information, such as names, phone numbers, and location data, was gathered, with boda boda riders, restaurant owners, and salon operators among those mandated to collect such data. These actors were required to collect data yet they had not been offered any training on how to protect the confidentiality of the data, what to do with the data they collected, or for how long they needed to keep the data.

47 *CIPESA, State of Internet Freedom in Africa 2019, https://cipesa.org/?wpfb_dl=307*

The data protection mishaps around COVID-19 bode badly for broader government-led digitalisation programmes, particularly those that entail collecting citizens' data. The haste in making regulations without proper public consultations, the hurried deployment of data collection solutions using opaque rules and practices, with no clearly defined purposes, limitations on use and storage periods, all presented major risks.

Uganda has legislation that provides guidance on protecting personal data, which should have been followed in the COVID-19 data collection exercises. However, the deficit in leadership and oversight by NITA-U meant that data collectors and processors could afford to ignore adhering to the principles of good data governance without fear of retribution. The situation was exacerbated by the lack of data protection regulations, which were only issued in mid-2021, two years after the Data Protection Act was enacted. The absence of meaningful parliamentary and public consultations on the various COVID-19 regulations issued by the government also hampered the opportunity to ensure that they embedded sufficient data rights safeguards. Ultimately, those regulations focused on addressing the health emergency and paid lip service to the protection of data rights. In turn, government agencies and their private sector collaborators did not fully adhere to the data protection principles in the collection of COVID-19 data.

United Nations experts cautioned that it was crucial that the use of surveillance technology to track the spread of the coronavirus be limited in terms of purpose and time, and that individual rights to privacy, non-discrimination, the protection of journalistic sources, and other freedoms, be rigorously protected.[48] They added that the use of such technology should "abide by the strictest protections and only be available according to domestic law that is consistent with international human rights standards."

There is therefore a need to push for the dismantling of the surveillance apparatus constituted to combat COVID-19's spread and provide for expiry of rights to process personal data collected by these systems. Moreover, authorities should issue transparency reports detailing the COVID-19-related surveillance activity, such as the tools and technologies used, state agencies and private entities involved, number of persons whose data were tracked, types of data collected, entities that accessed the data, and safeguards instituted to guard against misuse of the data and the surveillance apparatus.

48 *OSCE, COVID-19: Governments must promote and protect access to and free flow of information during pandemic, say international media freedom experts, March 19, 2020, https://www.osce.org/representative-on-freedom-of-media/448849*

Recommendations

Emergency situations including epidemics like COVID-19 create atmospheres that enable the unauthorised collection and use of personal data. Hence, it is imperative that relevant stakeholders including governments, civil society, academia, and the private sector take actions towards guaranteeing data protection and privacy of data subjects. Hence:

Government

- Should safeguard the right to privacy, as provided for in the Constitution and the Data Protection and Privacy Act, 2019, by sanctioning the collection, processing, and sharing of personal information in response to the COVID-19 pandemic for a specific purpose, namely, to curb the spread of the virus. This should include protection of the identity of the data subjects, and deletion or erasure of the personal data once it has served its purpose.
- Desist from mandating untrained and unregulated actors, such as boda boda riders and salon operators to collect personal data.
- Develop capacity among public institutions on engineering good data governance practices and respect for digital rights.

Telecommunication Companies and Internet service Providers

- Resist the urge to share identifiable personal data in their possession with government agencies without following provisions of the law, including the notification of data subjects.

Academia and Research organisations

- Should conduct evidence-based research and explore the implications of COVID-19 measures and their effects on the rights of individuals, especially data protection and privacy, and how infringement could affect the enjoyment of other fundamental human rights during and post-COVID-19 pandemic

Civil society and rights organisations

- Should continue engaging duty bearers, such the communications regulator, and the national identification and registration authority, on the need to respect peoples' right to data protection and privacy as enshrined in the Constitution and the Data Protection and Privacy Act, 2019.
- Should create awareness about and empower citizens on their rights to privacy and data protection.
- Should monitor, document, and expose cases of government infringement on fundamental human rights, especially the right to privacy and data protection.
- Should take collaborative litigation strategies to challenge any cases of data and privacy breaches by data collectors, controllers, and processors.

Individuals/data subjects

- Should demand for redress as provided in law, including requesting for erasure and/or remedies.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
+256 414 289 502
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org